





# DEVICE AND METHOD FOR OUTPUTTING RANDOM NUMBER SEQUENCE, PROGRAM, AND INFORMATION STORAGE MEDIUM

**Patent number:** JP2003140885  
**Publication date:** 2003-05-16  
**Inventor:** UMENO TAKESHI; ISHI MASAHIRO  
**Applicant:** JAPAN SCIENCE & TECH CORP; UMENO TAKESHI  
**Classification:**  
 - international: G06F7/58  
 - european:  
**Application number:** JP20010339429 20011105  
**Priority number(s):** JP20010339429 20011105

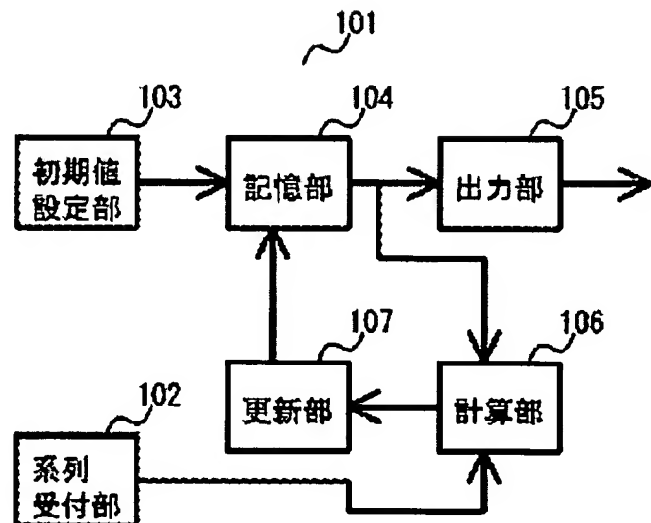
Also published as:

 EP1452959 (A1)  
 WO03040910 (A1)  
 WO03040910 (A1)  
 US2005033785 (A1)

Report a data error here

## Abstract of JP2003140885

**PROBLEM TO BE SOLVED:** To provide a device and the like for outputting a random number sequence. **SOLUTION:** A series receiving part 102 of a random number sequence outputting device 101 receives input of numerical value series, and an initial value setting part 103 receives input of an initial value and stores it to a storage part 104. An output part 105 outputs values every time when a new value is stored in the storage part 104, and a calculation part 106 applies a predetermined rational mapping to the value stored in the storage part 104 every time when the output part 105 outputs a value. A predetermined computing operation is applied to the mapped values and the values sequentially fetched from a numerical value series received by the series receiving part 102, for performing calculation. An updating part 107 stores the result value calculated by the calculation part 106 and updates it.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-140885

(P2003-140885A)

(43) 公開日 平成15年5月16日 (2003.5.16)

(51) Int.Cl.<sup>7</sup>

G 0 6 F 7/58

識別記号

F I

G 0 6 F 7/58

テ-マコ-ト\*(参考)

B

審査請求 有 請求項の数13 O L (全 8 頁)

(21) 出願番号 特願2001-339429(P2001-339429)

(22) 出願日 平成13年11月5日(2001.11.5)

(71) 出願人 396020800

科学技術振興事業団

埼玉県川口市本町4丁目1番8号

(71) 出願人 597044841

梅野 健

東京都小金井市貫井北町4-2-1 独立

行政法人通信総合研究所内

(72) 発明者 梅野 健

東京都小金井市貫井北町4-2-1 独立

行政法人通信総合研究所内

(74) 代理人 100095407

弁理士 木村 満 (外1名)

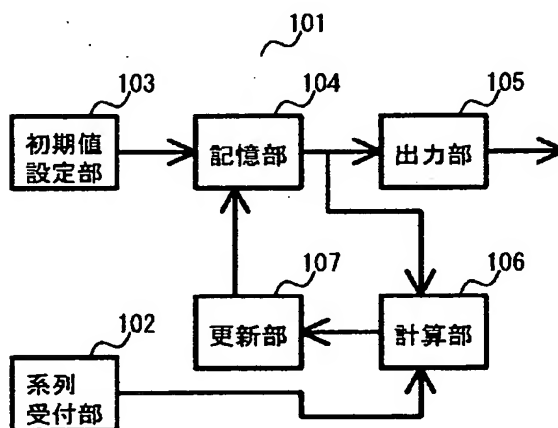
最終頁に続く

(54) 【発明の名称】 乱数列出力装置、乱数列出力方法、プログラムならびに、情報記録媒体

(57) 【要約】

【課題】 乱数列出力装置等を提供する。

【解決手段】 乱数列出力装置101の系列受付部102は、数値系列の入力を受け付け、初期値設定部103は、初期値の入力を受け付けてこれを記憶部104に記憶させ、出力部105は、記憶部104に新たな値が記憶される度にこれを出力し、計算部106は、出力部105が値を出力する度に、記憶部104に記憶された値に所定の有理写像を適用し、さらに、これと、系列受付部102により受け付けられた数値系列から順に取り出した値と、に所定の演算を施して、計算し、更新部107は、計算部106により計算された結果の値を記憶部104に記憶させて更新する。



## 【特許請求の範囲】

【請求項1】乱数列出力装置であって、系列受付部と、初期値設定部と、記憶部と、出力部と、計算部と、更新部と、を備え、

前記系列受付部は、数値系列の入力を受け付け、

前記初期値設定部は、初期値の入力を受け付けて、これを前記記憶部に記憶させ、

前記出力部は、前記記憶部に新たな値が記憶される度にこれを出力し、

前記計算部は、前記出力部が値を出力する度に、前記記憶部に記憶された値に所定の有理写像を適用し、さらに、これと、前記系列受付部により受け付けられた数値系列から順に取り出した値と、に所定の演算を施して、計算し、

前記更新部は、前記計算部により計算された結果の値を前記記憶部に記憶させて更新することを特徴とするもの。

【請求項2】請求項1に記載の乱数列出力装置であって、

前記所定の有理写像は、整数 $a$ に対して

$$T(a, \cos \theta) = \cos(a\theta)$$

により定義される $a$  ( $a \geq 2$ ) 次のチェビシェフ写像 $T(a, \cdot)$ であることを特徴とするもの。

【請求項3】請求項2に記載の乱数列出力装置であって、

前記記憶部は、当該値を所定ビット数の固定小数点表現で記憶することを特徴とするもの。

【請求項4】請求項3に記載の乱数列出力装置であって、

当該所定の演算は、当該数値系列から順に取り出した値が所定の値である場合、当該値の所定ビット数の固定小数点表現の所定位置のビットを反転させることを特徴とするもの。

【請求項5】請求項4に記載の乱数列出力装置であって、

当該数値系列は、長さ $T$ であって、0または1の値をとる2値系列（ゴールド符号、M系列、ペーカー系列を含む。）を繰り返したものであり、

当該所定位置のビットは、当該固定小数点表現の最下位ビットであり、

当該所定の値は1であることを特徴とするもの。

【請求項6】値を記憶する記憶部を用いる乱数列出力方法であって、系列受付工程と、初期値設定工程と、出力工程と、計算工程と、更新工程と、を備え、

前記系列受付工程では、数値系列の入力を受け付け、

前記初期値設定工程では、初期値の入力を受け付けて、これを前記記憶部に記憶させ、

前記出力工程では、前記記憶部に新たな値が記憶される度にこれを出力し、

前記計算工程では、前記出力工程にて値が出力される度

に、前記記憶部に記憶された値に所定の有理写像を適用し、さらに、これと、前記系列受付工程にて受け付けられた数値系列から順に取り出した値と、に所定の演算を施して、計算し、

前記更新工程では、前記計算工程にて計算された結果の値を前記記憶部に記憶させて更新することを特徴とする方法。

【請求項7】請求項6に記載の乱数列出力方法であって、

前記所定の有理写像は、整数 $a$ に対して

$$T(a, \cos \theta) = \cos(a\theta)$$

により定義される $a$  ( $a \geq 2$ ) 次のチェビシェフ写像 $T(a, \cdot)$ であることを特徴とする方法。

【請求項8】請求項7に記載の乱数列出力方法であって、前記初期値設定工程、および、前記更新工程では、前記記憶部に当該値を所定ビット数の固定小数点表現で記憶させることを特徴とする方法。

【請求項9】請求項8に記載の乱数列出力方法であって、

20 当該所定の演算は、当該数値系列から順に取り出した値が所定の値である場合、当該値の所定ビット数の固定小数点表現の所定位置のビットを反転させることを特徴とする方法。

【請求項10】請求項9に記載の乱数列出力方法であって、

当該数値系列は、長さ $T$ であって、0または1の値をとる2値系列（ゴールド符号、M系列、ペーカー系列を含む。）を繰り返したものであり、

当該所定位置のビットは、当該固定小数点表現の最下位ビットであり、

当該所定の値は1であることを特徴とする方法。

【請求項11】コンピュータを、請求項1から5のいずれか1項に記載の乱数列出力装置として機能させることを特徴とするプログラム。

【請求項12】コンピュータに、請求項6から10のいずれか1項に記載の乱数列出力方法を実行させることを特徴とするプログラム。

40 【請求項13】請求項11または12に記載のプログラムを記録したことを特徴とするコンピュータ読取可能な情報記録媒体（コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、乱数列出力装置、乱数列出力方法、これらを実現するためのプログラム、ならびに、当該プログラムを記録したコンピュータ読取可能な情報記録媒体に関する。

【0002】

【従来の技術】従来から、チェビシェフ多項式を用いたカオス写像による乱数列の生成技術が知られている。これは、整数 $a$ に対して

$$T(a, \cos \theta) = \cos(a\theta)$$

により定義される $a$  ( $a \geq 2$ ) 次のチェビシェフ写像 $T(a, \cdot)$ を用いた漸化式

$$x_{i+1} = T(a, x_i) \quad (i \geq 0)$$

に対して、初期値 $x_0$  ( $-1 < x_0 < 1$ ) を与えることにより得られる系列

$$x_0, x_1, x_2, \dots$$

を擬似乱数列とするものである。また、チェビシェフ写像以外にも、種々の有理関数を用いる手法が提案されている。

【0003】この技術によれば、漸化式の計算を有理数で行えば、周期のない擬似乱数列が得られ、生成される乱数の分布が解析的に表現できることがわかっている。

【0004】

【発明が解決しようとする課題】しかしながら、無限精度の有理数表現にて漸化式を計算する場合であっても、様々な擬似乱数の生成手法が実現されることが望ましい。

【0005】また、漸化式の計算を所定の精度の固定小数点数表現や浮動小数点数表現により行った場合には、得られる系列には周期が現れてしまい、その周期が短い場合がある、という問題が生じていた。

【0006】さらに、生成される系列の分布が、上記の解析的に表現される分布とは異なり、特定の値に偏った分布となってしまう場合がある、という問題が生じていた。

【0007】本発明は、このような問題を解決するための手法であって、乱数列出力装置、乱数列出力方法、これらを実現するためのプログラム、ならびに、当該プログラムを記録したコンピュータ読取可能な情報記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【0009】本発明の第1の観点に係る乱数列出力装置は、系列受付部と、初期値設定部と、記憶部と、出力部と、計算部と、更新部と、を備え、以下のように構成する。

【0010】すなわち、系列受付部は、数値系列の入力を受け付ける。

【0011】一方、初期値設定部は、初期値の入力を受け付けて、これを記憶部に記憶させる。

【0012】さらに、出力部は、記憶部に新たな値が記憶される度にこれを出力する。

【0013】そして、計算部は、出力部が値を出力する度に、記憶部に記憶された値に所定の有理写像を適用

し、さらに、これと、系列受付部により受け付けられた数値系列から順に取り出した値と、に所定の演算を施して、計算する。

【0014】一方、更新部は、計算部により計算された結果の値を記憶部に記憶させて更新する。

【0015】また、本発明の乱数列出力装置において、所定の有理写像は、2次以上のチェビシェフ写像であるように構成することができる。

【0016】また、本発明の乱数列出力装置において、記憶部は、当該値を所定ビット数の固定小数点表現で記憶するように構成することができる。

【0017】また、本発明の乱数列出力装置において、当該所定の演算は、当該数値系列から順に取り出した値が所定の値である場合、当該値の所定ビット数の固定小数点表現の所定位置のビットを反転させるように構成することができる。

【0018】また、本発明の乱数列出力装置において、当該数値系列は、長さ $T$ であって、0または1の値をとる2値系列（ゴールド符号、M系列、ペーカー系列を含む。）を繰り返したものであり、当該所定位置のビットは、当該固定小数点表現の最下位ビットであり、当該所定の値は1であるように構成することができる。

【0019】本発明の他の観点に係る乱数列出力方法は、値を記憶する記憶部を用い、系列受付工程と、初期値設定工程と、出力工程と、計算工程と、更新工程と、を備え、以下のように構成する。

【0020】すなわち、系列受付工程では、数値系列の入力を受け付ける。

【0021】一方、初期値設定工程では、初期値の入力を受け付けて、これを記憶部に記憶させる。

【0022】さらに、出力工程では、記憶部に新たな値が記憶される度にこれを出力する。

【0023】そして、計算工程では、出力工程にて値が出力される度に、記憶部に記憶された値に所定の有理写像を適用し、さらに、これと、系列受付工程にて受け付けられた数値系列から順に取り出した値と、に所定の演算を施して、計算する。

【0024】一方、更新工程では、計算工程にて計算された結果の値を記憶部に記憶させて更新する。

【0025】また、本発明の乱数列出力方法において、所定の有理写像は、2次以上のチェビシェフ写像であるように構成することができる。

【0026】また、本発明の乱数列出力方法において、初期値設定工程、および、更新工程では、記憶部に当該値を所定ビット数の固定小数点表現で記憶させるように構成することができる。

【0027】また、本発明の乱数列出力方法において、当該所定の演算は、当該数値系列から順に取り出した値が所定の値である場合、当該値の所定ビット数の固定小数点表現の所定位置のビットを反転させるように構成す

ることができる。

【0028】また、本発明の乱数列出力方法において、当該数値系列は、長さTであって、0または1の値をとる2値系列（ゴールド符号、M系列、ペーカー系列を含む。）を繰り返したものであり、当該所定位置のビットは、当該固定小数点表現の最下位ビットであり、当該所定の値は1であるように構成することができる。

【0029】本発明の他の観点に係るプログラムは、コンピュータ（ASIC（Application Specific Integrated Circuit）、DSP（Digital Signal Processor）、FPGA（Field Programmable Gate Array）を含む。）を、上記の乱数列出力装置として機能させ、または、コンピュータに、上記の乱数列出力方法を実行させるように構成する。

【0030】また、本発明のプログラムは、コンピュータ読取可能な情報記録媒体（コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、デジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）に記録することができる。

【0031】本発明のプログラムを、記憶装置、計算装置、出力装置、通信装置などを備える汎用コンピュータ、携帯電話機、PHS（Personal Handyphone System）装置、ゲーム装置などの携帯端末、並列計算機などの情報処理装置、ASIC、DSP、FPGAなどで実行することにより、上記の乱数列出力装置、ならびに、乱数列出力方法を実現することができる。

【0032】また、これらの装置とは独立して、本発明の情報記録媒体を店舗等で配布、販売したり、本発明のプログラムそのものをコンピュータ通信網を介して配布、販売したりすることができる。

【0033】

【発明の実施の形態】以下に本発明の実施形態を説明する。なお、以下にあげる実施形態は、説明のためのものであり、本発明の範囲を制限するものではない。したがって、当業者であれば、これらの各要素または全要素を、これと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も、本発明の範囲に含まれる。

【0034】（発明の実施の形態）図1は、本発明の実施の形態に係る乱数列発生装置の概要構成を示す模式図である。図2は、当該乱数列発生装置にて実行される乱数列発生方法の処理の流れを示すフローチャートである。以下、これらの図を参照して説明する。

【0035】乱数列出力装置101は、系列受付部102と、初期値設定部103と、記憶部104と、出力部105と、計算部106と、更新部107と、を備える。

【0036】まず、系列受付部102は、数値系列の入力を受け付ける（ステップS201）。当該数値系列は、典型的には、ゴールド符号、M系列、ペーカー系列

等の2値系列を繰り返したものである。ゴールド符号とM系列は、周期 $T = 2^n - 1$ の0または1の値からなる擬似乱数列である。

【0037】なお、系列受付部102は、ひとまず、長さTの数値系列を整数値として受け付けて、当該整数値を記憶しておき、後述するように、その整数値の最下位ビットを順に取得して利用した後、当該整数値を巡回シフト（「ローテート」「シフト回転」ともいう。）するようにしてもよい。

10 【0038】次に、初期値設定部103は、初期値の入力を受け付けて（ステップS202）、これを記憶部104に記憶させる（ステップS203）。

【0039】記憶部104は、典型的には、値を所定ビット数の固定小数点表現で記憶する。図3に、Nビットの固定小数点表現を採用した場合の様子を示す。本図には、0～1の間の固定小数点数の場合を図示してある。最上位ビットから最下位ビットまで順に $b_0$ 、 $b_1$ 、 $b_2$ 、 $\dots$ 、 $b_{n-1}$ と置くと、そのそれぞれは、1または0の値をとる。この固定小数点表現は、

20  $\sum_{i=0}^{n-1} (1/2)^{i+1} b_i$   
という0以上1未満の数値に対応付けられる。

【0040】なお、多くの計算機においては、この固定小数点表現を符号無し整数と見ると、

$\sum_{i=0}^{n-1} 2^{n-1-i} b_i$   
という整数値に対応付けられる。

【0041】このほか、 $-1 \sim 1$ の間の固定小数点数の場合は、 $b_0 \sim b_{n-1}$ のいずれか一つ（典型的には $b_0$ ）を符号ビットとし、残りで固定小数点数を表現することが多い。たとえば、 $b_0$ を符号ビットとした場合、 $b_0 \sim b_{n-1}$ による固定小数点表現は、 $b_0 = 0$ の場合は、

30  $\sum_{i=1}^{n-1} (1/2)^i b_i$   
 $b_0 = 1$ の場合は、  
 $-\sum_{i=1}^{n-1} (1/2)^i b_i$   
に、それぞれ対応することになる。

【0042】さらに、出力部105は、記憶部104に新たな値が記憶される度にこれを出力する（ステップS204）。

【0043】そして、計算部106は、出力部105が値を出力する度に、記憶部104に記憶された値に所定の有理写像を適用し（ステップS205）、さらに、これと、系列受付部102により受け付けられた数値系列から順に取り出した値と、に所定の演算（以下「ハーネシング」という。）を施して、計算する（ステップS206）。

【0044】典型的には、所定の有理写像は、2次以上のチェビシェフ写像である。図4は、チェビシェフ写像の様子を示すグラフである。チェビシェフ写像は、多項式で表すと、以下のように表現できる。

$$T(0, x) = 1$$

50  $T(1, x) = x$

$$T(2, x) = 2x^2 - 1$$

$$T(3, x) = 4x^3 - 3x$$

【0045】チェビシェフ多項式 $v = T(a, x)$ は、いずれも、開区間 $-1 < x < 1$ を開区間 $-1 < y < 1$ に写像する有理写像である。

【0046】本図には、次数2から5のチェビシェフ多項式が、 $v = T(2, x)$ 、 $v = T(3, x)$ 、 $v = T(4, x)$ 、 $v = T(5, x)$ の形式でグラフ表示されている。横軸がx軸、縦軸がy軸である。

【0047】また、ハーネシングは、典型的には、当該数値系列から順に取り出した値が所定の値である場合、当該値の所定ビット数の固定小数点表現の所定位置のビットを反転させるものである。すなわち、当該所定の値が1である場合に、最下位ビット $b_{n-1}$ の値を反転する演算である。

【0048】上述のように、M系列等を起源とする数値系列からは、0または1の値が得られるが、この「0または1の値」と、記憶部106に記憶された固定小数点表現を「符号無し整数」として見た場合に、両者の排他的論理和(exclusive or)を計算して、これを記憶部106に記憶させればよい。

【0049】なお、最下位ビットではなく、他の位置のビットと排他的論理和をとるような実施形態を採用することもできる。ただし、符号ビット以外のビットとすることが望ましい。

【0050】一方、更新部107は、計算部106により計算された結果の値を記憶部104に記憶させて更新し(ステップS207)、ステップS204に戻る。

【0051】なお、ハーネシングの演算は、このほかの態様であってもよい。たとえば、上記の固定小数点表現によれば、 $b_0 \sim b_{n-1}$ の値がどのようになっているとも、これが表現する固定小数点数は $-1 \sim 1$ の範囲に納まるので、様々なビット演算等を考えることができる。たとえば、以下のような演算である。

・当該数値系列から順に取り出した値(0または1)だけ当該固定小数点表現のビット列を巡回シフトする。

・当該数値系列から順に取り出した値(0または1)を、当該固定小数点表現のビット列を「符号無し整数」として見たものに加算する。

・当該数値系列から順に取り出した値(0または1)を、当該固定小数点表現のビット列を「符号無し整数」として見たものから減算する。

・当該数値系列から順に取り出した値(0または1)があらかじめ定めた値(たとえば1)である場合、所定の整数 $p$ 、 $q$  ( $0 \leq p, q \leq N-1$ )について、ビット $b_p$ の値とビット $b_q$ の値とを交換する。

【0052】これらについては、得られる系列の周期を検討した上で、いずれの演算を採用するかを決めることができる。

【0053】(実験の結果)図5は、無限精度の有理数

表現でチェビシェフ写像により系列を生成した場合の系列分布を表示したグラフである。

【0054】図6は、8ビット精度で、ハーネシングを行わなかった場合の系列分布を示すグラフである。図7は、8ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。図8は、12ビット精度で、ハーネシングを行わなかった場合の系列分布を示すグラフである。図9は、12ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。図10は、16ビット精度で、ハーネシングを行わなかった場合の系列分布を示すグラフである。図11は、16ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。

【0055】これらを比較してみると、ハーネシングを行わなかった場合の系列分布には、大きな偏りがあり、無限精度の有理数表現を用いた場合との分布には大きな違いがあるが、本実施形態の手法を用いると、無限精度の有理数表現を用いた場合と分布が類似していることがわかり、良い擬似乱数が得られていることがわかる。

【0056】また、出力される系列の周期について調べると、本実施形態のようにハーネシングを行うことにより、多くの場合は周期が数倍から数十倍に長くなることがわかる。したがって、より望ましい擬似乱数列が得られることになる。

【0057】

【発明の効果】以上説明したように、本発明によれば、乱数列出力装置、乱数列出力方法、これらを実現するためのプログラム、ならびに、当該プログラムを記録したコンピュータ読取可能な情報記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る乱数列発生装置の概要構成を示す模式図である。

【図2】乱数列発生装置にて実行される乱数列発生方法の処理の流れを示すフローチャートである。

【図3】Nビットの固定小数点表現を採用した場合の様子を示す説明図である。

【図4】チェビシェフ写像の様子を示すグラフである。

【図5】無限精度の有理数表現でチェビシェフ写像により系列を生成した場合の系列分布を表示したグラフである。

【図6】8ビット精度で、ハーネシングを行わなかった場合の系列分布を示すグラフである。

【図7】8ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。

【図8】12ビット精度で、ハーネシングを行わなかった場合の系列分布を示すグラフである。

【図9】12ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。

【図10】16ビット精度で、ハーネシングを行わな

った場合の系列分布を示すグラフである。

【図11】16ビット精度で、上記実施形態を採用した場合の系列分布を示すグラフである。

【符号の説明】

101 乱数出力装置

102 系列受付部

\* 103 初期値設定部

104 記憶部

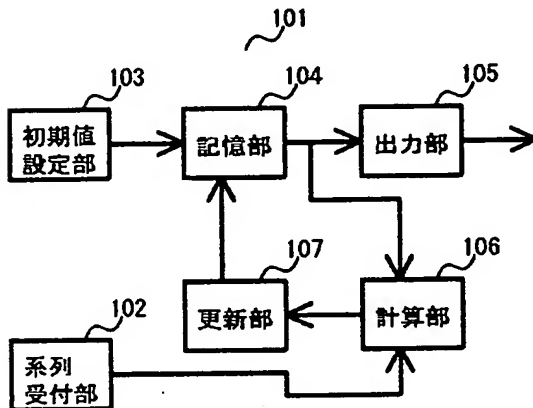
105 出力部

106 計算部

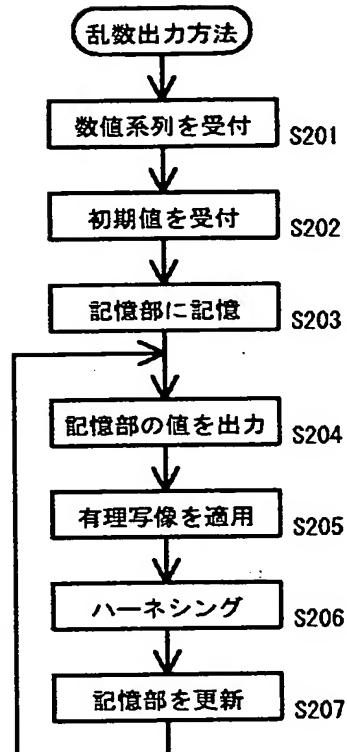
107 更新部

\*

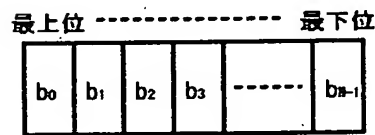
【図1】



【図2】



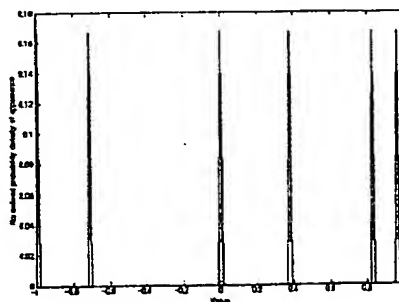
【図3】



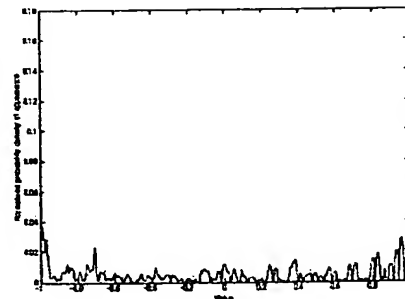
$$\sum_{n=0}^{N-1} (1/2)^{n+1} b_n \quad \text{固定小数点表現}$$

$$\sum_{n=0}^{N-1} 2^{N-1-n} b_n \quad \text{整数表現}$$

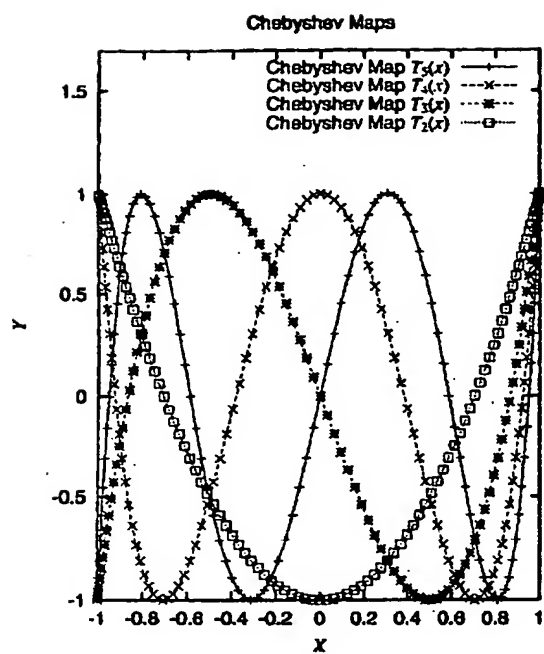
【図6】



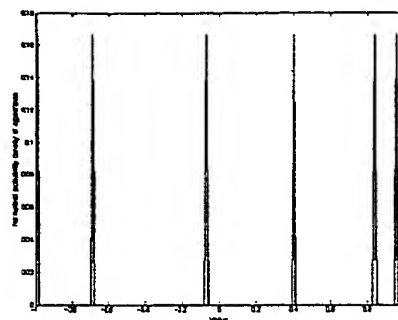
【図7】



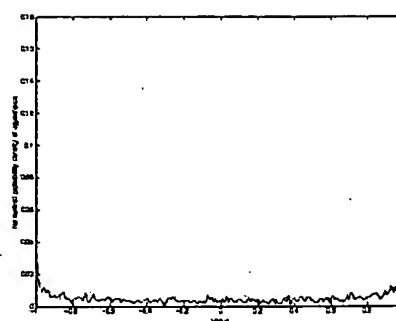
【図4】



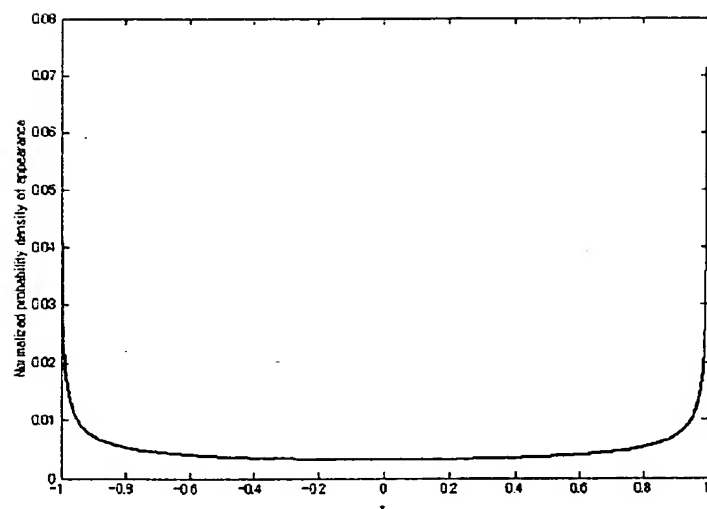
【図8】



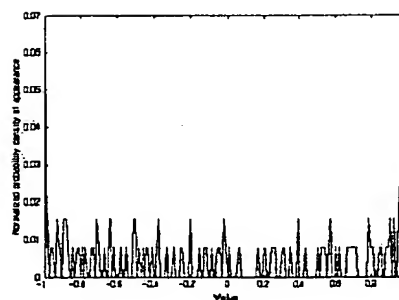
【図9】



【図5】

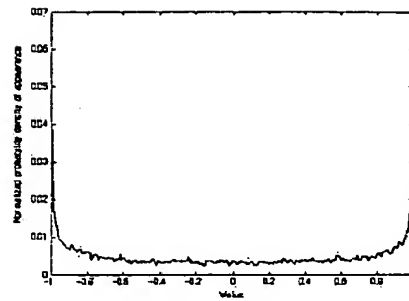


【図10】





【図11】



---

フロントページの続き

(72)発明者 石 聖弘  
東京都渋谷区渋谷 1-20-1 三進ビル4  
階 科学技術振興事業団内